

# IdentityMinder<sup>®</sup> eProvision

---

Comprehensive Identity Management and  
Resource Provisioning

---

**Netegrity Technical White Paper**

January 20, 2004

## Table of Contents

Introduction .....	3
IdentityMinder eProvision: How it Works .....	3
IdentityMinder eProvision: Features .....	4
Policy Based Resource Provisioning.....	5
Dynamic Business Rules Engine .....	6
Delegated Administration.....	6
User Self Service .....	7
Password Management.....	7
Resource Connectors (ePMs) .....	9
Data Synchronization .....	10
Reverse (Bi-Directional) Synchronization .....	11
Progress Monitoring.....	12
Auditing .....	12
Reporting .....	13
Summary.....	14

## Introduction

As corporations extend their computing power to more users, they must ensure that the appropriate resources are available. Not only must resources be available to all users who need them, both inside and outside the company, they must be made available quickly and efficiently. At the same time, corporations must ensure that their resources are never at risk. Balancing the conflicting demands between making resources open and available yet maintaining a controlled and secure environment is one of the most difficult problems businesses must solve.

Netegrity IdentityMinder® IdentityMinder eProvision is the enterprise solution designed specifically to balance these demands. With IdentityMinder eProvision, corporations can cost-effectively support up to hundreds of thousands of users by managing their identities. Once a user has their IdentityMinder eProvision identity, whether it is a company officer, a business partner, an employee, or a casually interested consumer, their access to corporate resources can be managed.

Not only does IdentityMinder eProvision provide the best solution for managing users, the solution is cost-effective and designed for use by the entire business, not just the high-level security administrators. IdentityMinder eProvision is:

- ❑ *Easy-to-use* – The administrative and end user Web interface is intuitive and easy to learn.
- ❑ *Scalable* – Administrator and access roles provide access scalability at a level unattainable with today's standard attribute- or group-based schemes. IdentityMinder eProvision can support any corporation size, up to millions of users.
- ❑ *Extensible* – IdentityMinder eProvision provides an SDK that, when combined with its out-of-the-box functionality, allows companies extend IdentityMinder eProvision to work directly with any other business applications. As a result, IdentityMinder eProvision is capable of meeting user management requirements the corporation has now and in the future.
- ❑ *Customizable* – IdentityMinder eProvision end-user operations can be seamlessly integrated into the corporate interface. The out-of-the-box functions and user interfaces are designed to be easily customized to your company's look and feel.
- ❑ *Flexible* – IdentityMinder eProvision supports a wide range of connectors to target systems (e.g. HR, ERP, OS, etc) and includes a powerful connector development wizard called the Xpress tool that allows companies to develop custom connectors to manage users on virtually any target application.
- ❑ *Cost-effective* – Scalability in administration drives down overall IT costs so substantially that a return-on-investment can be realized in a relatively short period of time. For a detailed perspective on the ROI for Identity Management and Resource Provisioning, see the Gartner ROI tool available on the Netegrity Web site (<http://www.netegrity.com>).

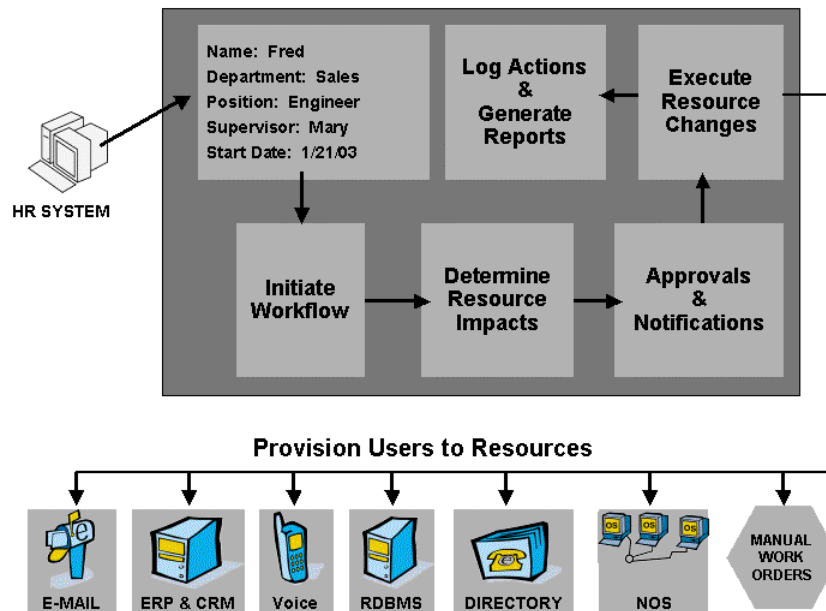
## IdentityMinder Provisioning Edition: How it works

The diagram below provides a quick overview of a common identity management and provisioning use case that illustrates how IdentityMinder eProvision can be utilized in an enterprise environment. In this example, IdentityMinder eProvision is configured to manage the process of creating an identity for a new employee and then provisioning them with the resources needed to be successful in their new position.

In many companies, after a decision is made to hire a new employee, an HR manager creates a new record for the employee in an HR system (e.g. PeopleSoft). With eProvision, a connector to the HR system can be configured to detect new records, or changes made to existing records that are then put through the provisioning process. This may trigger a workflow process that helps manage all of the identity management and provisioning tasks that may be needed to allocate the employee all of the resources needed to perform their job. After gaining the necessary approvals, the new employee record is entered into the IdentityMinder eProvision user store.

The addition of the new employee to the IdentityMinder eProvision user store causes a notification to be sent to the provisioning engine, which then determines the resource impacts for this new employee by evaluating the provisioning policies (rules) that are configured in the system. After determining the resource impact for the new employee, the provisioning engine dynamically assembles a list of provisioning tasks to execute (e.g. Create Windows account, Create email account, etc. etc.). At this point, each individual provisioning task may also have an approval, notification, and escalation process associated with it. This ensures that resource owners have the opportunity to intervene if necessary before any actions are taken on the resource they manage.

Finally, after gaining the appropriate approvals, the provisioning engine dispatches requests to each resource connector to create an account on each target system that the new employee needs to have access to. Each provisioning task and event is recorded and written to an audit database to ensure that all actions are logged. Upon successful completion of all provisioning tasks, the new employee now has access to all of the resources needed to be successful in their new position.



**Figure 1: IdentityMinder eProvision: how it works**

## IdentityMinder® eProvision: Features

All IdentityMinder eProvision features are designed to increase the efficiency of business operations throughout the corporation. By increasing the efficiency of managing users, all users benefit from gaining a more timely response to resources they need. IdentityMinder eProvision goes even further: by using its automation features in conjunction with its user management features, administrators can increase the efficiency of the business operations too.

IdentityMinder eProvision offers a comprehensive user management and resource provisioning solution. With IdentityMinder eProvision, businesses gain a powerful set of capabilities that increase productivity and security, while reducing the risk of unauthorized access to corporate resources. IdentityMinder eProvision has the following capabilities:

- ☐ Policy-based resource provisioning
- ☐ Dynamic Business Rules Engine
- ☐ Password management (reset and synchronization)
- ☐ Resource connectors (ePMs)
- ☐ Data synchronization
- ☐ Active progress monitoring

Each of these features is described in more detail in the sections that follow.

## Policy Based Resource Provisioning

IdentityMinder eProvision provides a robust, cost-effective means for automating the process of managing user accounts and profiles in enterprise and legacy resources. It also provides an efficient mechanism for automating manual employee provisioning tasks like providing a desk and office phone for a new employee.

The provisioning process begins by loading input about a user into a digital profile that contains all of the user's business and resource information. The initial population of user profile data may originate from an authoritative HR feed like PeopleSoft, or from a new user being entered directly from a Web-based user interface. Each rule in the provisioning engine examines the contents of one or more business attributes and makes a provisioning decision based on the value of the attributes.

Resource allocation decisions made by the provisioning engine's dynamic business rules engine can determine all aspects of the user's access to a resource. For example, once the rules determine that the user should get access to a resource, they can also determine the correct server, appropriate security group memberships, the structure of the user's ID (to conform to a company standard), set all of the access control settings, and administer any other options available relative to the user's account on the target system.

The results of each provisioning decision are stored in each user's digital profile in the master identity store. Managed by IdentityMinder eProvision, provisioning rules can be designed to evaluate data from the user's business attributes as well as resource-specific attributes to determine the overall resource impact for a given user. IdentityMinder eProvision provides a robust GUI-based rules designer tool that simplifies the process of defining provisioning policies.

Finally, the importance of the iterative approach is that the system can make sure that all rules are evaluated more than once, to ensure that rules that are dependent on specific data being available can be evaluated with no concern for the sequence of the rule execution. The solution is able to map to a customer's existing business processes, and even enables allowing multiple groups within the company have their own sets of rules.

With IdentityMinder eProvision, Netegrity has delivered an enterprise-class identity management and resource provisioning solution that can meet the needs of the most demanding and fragmented IT, network, and application environments found in large enterprises. The Netegrity approach allows companies to create order on a global scale but allows the individual operating units (e.g. departments or teams) the autonomy and control that they need.

## Dynamic Business Rules Engine

The built in business rules engine automatically assesses the impact of a business change to the IT infrastructure and dynamically organizes the required activities into a series of provisioning tasks to execute based on provisioning policies. This dramatically simplifies the development and maintenance of provisioning processes by generating those processes on-the-fly.

IdentityMinder eProvision's dynamic business rules engine generates the set of provisioning tasks to execute for each business change on the fly. This eliminates the need to write predefined workflows and allows the provisioning engine to dynamically assemble a set of provisioning tasks through rule definitions and allocation policies. It also means that by adding a new policy, or updating the data used by existing policies, different results may occur from a resource allocation standpoint.

The dynamic business rules engine is integrated into all aspects of the product including process scheduler and session manager. This allows the system a more fine-grained and natural ability to handle approvals, escalations, notifications, and data gathering. Each provisioning rule can be evaluated and processed as the provisioning transaction develops instead of needing to happen ahead of time.

This also increases the system's dynamics. The generation of activities for a given business change are dynamically generated and can be refined in real time as conditions change and variables acquire values. In the traditional approach used by several products, the transaction would have to be cancelled and restarted in order to handle conditions that change in real time. This even includes connectivity failures to target systems.

The tight integration of the dynamic business rules engine with the other core processing components also means that manual tasks, tasks that create work orders and are handled by people, can be uniformly integrated into a provisioning transaction. In fact, when the provisioning engine selects tasks as part of a provisioning transaction it does not differentiate between manual or automatic tasks. Manual and automated provisioning tasks can be mixed freely to meet the demands of virtually any business process, and either type can depend on the other type for data or services with no restrictions. Approvals, monitoring, escalation, feedback, etc. are applied equally to both types as well.

## Delegated Administration

User administration is often one of the most time consuming tasks for administrators, yet it is not inherently difficult. Highly valued system administrators are often wasted on completing tasks that almost anyone can do. With IdentityMinder eProvision, administrators can selectively delegate user administration and profile management down to business units, remote offices, partner/supplier administrators or even end users (for unattended, self-service) through a browser-based interface. This reduces load/dependency on centralized IT for user management and provisioning activities.

Once administrators delegate user management tasks, multiple benefits result:

- ☐ Companies need fewer administrators for user management as business users and partners take on the responsibility for managing access for themselves.
- ☐ The highly valued administrators can focus on the tasks no one else can do, such as defining the corporate security standards and policies and implementing a strong, central security infrastructure.
- ☐ Users waiting for administrators to fulfill requests don't have to wait as long to get their needs met.

With IdentityMinder eProvision, administrators can securely delegate tasks to the person most suited for completing them. In a company with distinct organizational units, a central administrator can designate that managers within the company's departments perform day-to-day user management tasks. If they choose, administrators can also enable that users perform tasks on their own. For example, if users could do their own account registration, this reduces an enormous amount of work for the administrator while at the same time improves end-user service significantly.

## User Self Service

To provide a high quality user experience for people inside and outside the company, corporations need to extend the ability to complete some tasks without requiring human intervention. Usually, corporations want external users to be able to perform basic tasks rapidly, such as create an account for themselves or become part of a general interest group. IdentityMinder eProvision provides administrators with the capability of providing users with self-service functions without jeopardizing corporate resources.

There are several types of self-service activities that are included with IdentityMinder eProvision, including: new user registration, user profile management, and forgotten password reset services. Each of these services is flexible and can be configured to meet specific business needs.

For end user profile management, users can be delegated specific profile management tasks that allow them to self-manage certain attributes that are stored in the user directory (e.g. address, phone number, etc). An administrator can pick and choose what attributes are "editable" by end users and optionally configure a workflow approval process for changes to their profile that might require manager approval. In addition, the provisioning engine can be configured to detect attribute changes to a user's profile and optionally synchronize these changes with other target systems that are managed by the provisioning engine.

In the case when a user may have forgotten their primary password and require a self service facility to reset it, IdentityMinder eProvision offers a self-service password reset service. This feature is typically exposed from via a standard Web UI that prompts the user to answer a series of challenge-response questions (e.g. mother's maiden name) before they are allowed to reset their password. At this point, the system can be configured with password policies to ensure that users select "strong" passwords that are difficult to break. Empowering end-users in this way frees up System Administrators and Help Desk staff from the burdens and costs associated with resetting forgotten passwords. This translates to substantial savings in the time and dollars dedicated to managing this pervasive end-user problem.

## Password Management

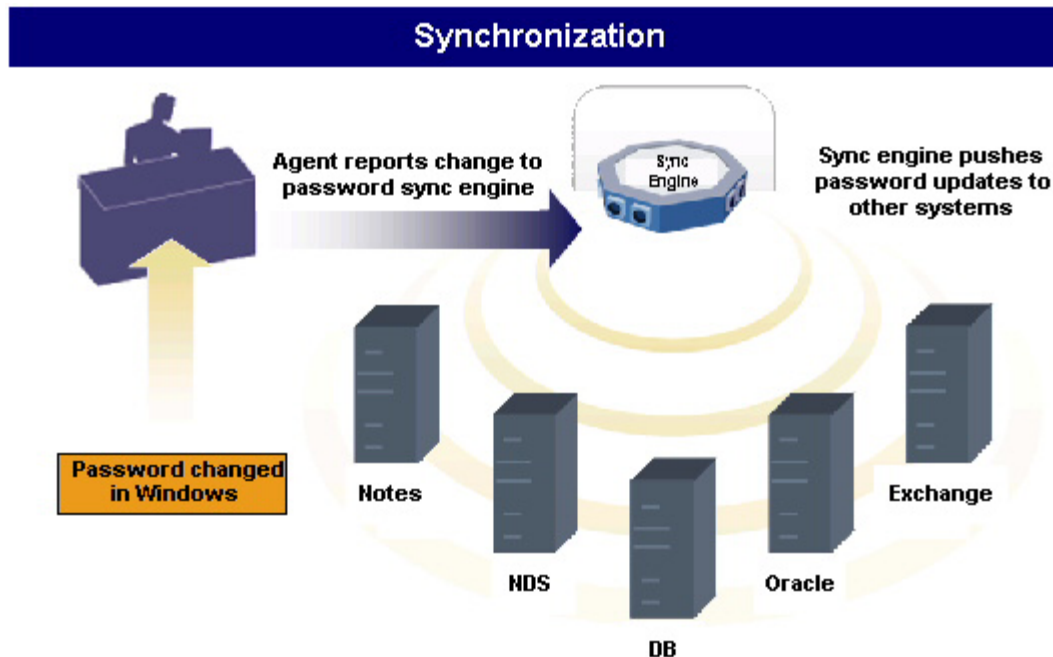
People with access to shared network resources, can inadvertently compromise organizational security by:

- ☐ Choosing weak passwords that can be easily remembered but are easily guessed
- ☐ Writing down passwords and security token PINs, and storing them in public view
- ☐ Emailing passwords and PINs to themselves at work and at home
- ☐ Sharing passwords, PINs, and security tokens with co-workers who are waiting for system access

Personnel who are more careful may forget their passwords, PINs, or security tokens and frequently call the help desk. IT staff must focus a significant amount of time on basic password and security token management, creating "downtime" while new personnel wait for user accounts to be set up.

Netegrity offers customers a sleek solution for managing end-user passwords via the password management capabilities offered by IdentityMinder eProvision, which includes both password synchronization and reset. The option delivers a total password management solution with the strength needed to reduce costs while increasing corporate security.

IdentityMinder eProvision's password synchronization engine provides a robust and secure mechanism that manages the synchronization of passwords across a range of systems. When a user's password changes on one system the password synchronization engine updates the user's password on all the other systems where the user has an account.



**Figure 2 – Password Synchronization**

Unlike other security solutions, Netegrity's password synchronization engine requires no code at the desktop. Instead, the engine relies on a centralized approach to detecting password changes, by utilizing the existing security packages of your system. This approach does not introduce new security risks in the form of a proprietary database or a new sign-on mechanism, nor does it increase your system's required day-to-day maintenance.

The synchronization engine synchronizes password changes between all major operating systems including OS/390, AS/400, Windows NT/2000, Windows 95/98, UNIX, Novell NetWare, LDAP and ODBC compliant database and is fully compatible with security tools such as RACF, CA-ACF2, CA-Top Secret, etc.

The password synchronization service can be used in several ways with eProvision. The most common way is as part of a reduced sign-on strategy. This typically involves giving users the same ID and passwords on all systems so that the user is not burdened by the need to remember different user ID and password combinations. This is helpful in many situations because it helps eliminate the tendency for users to write down their IDs and passwords in convenient but insecure places.

Companies that follow a reduced sign-on strategy usually choose to change passwords frequently as an added security measure. Password synchronization will help make it simpler for users since they will only need to reset the password on one system and the synchronization engine propagates it out to any other system where the user has an account.

Sometimes, companies will require that users have different IDs and passwords or at least passwords on each system. Another reason for allowing differing passwords is that some systems have different password policies that may reject a synchronization request from another system if the password being propagated does not meet the password policy for a given target system.

For example, on System A, the minimum password length may be 8 characters while on System B, the maximum password length may be 6 characters. IdentityMinder eProvision provides a password capability called harmonization that can take care of deriving the correct password for each system based on the original password. It's easy for the password administrator to create the formula so that user's will know what their password will be on each system.

## Resource Connectors (ePMs)

A key concern of organizations implementing a resource provisioning solution is creating the connectivity to the myriad IT systems that exist in the organization. Netegrity offers a large set of connectors to common applications within the enterprise.

ePMs serve as the primary conduit for communication between the provisioning engine and managed systems within the IT infrastructure. They provide the communication channel for translating business changes that may be initiated through user account modifications in IdentityMinder eProvision to the corresponding account changes for each specific platform or resource that a user has been provisioned to. When a request to implement a business change is entered via the IdentityMinder eProvision system (e.g. synchronizing a user attribute change from IdentityMinder eProvision out to a target system), the ePM for each system affected is notified. Each ePM, in turn, triggers the mechanism to execute the required IT change in the IT system. Typically, an ePM contains a component that interacts with the provisioning engine and a component that configures the IT system. These two components interact via a COM or Java interface and may function in an agent-less or agent-based mode.

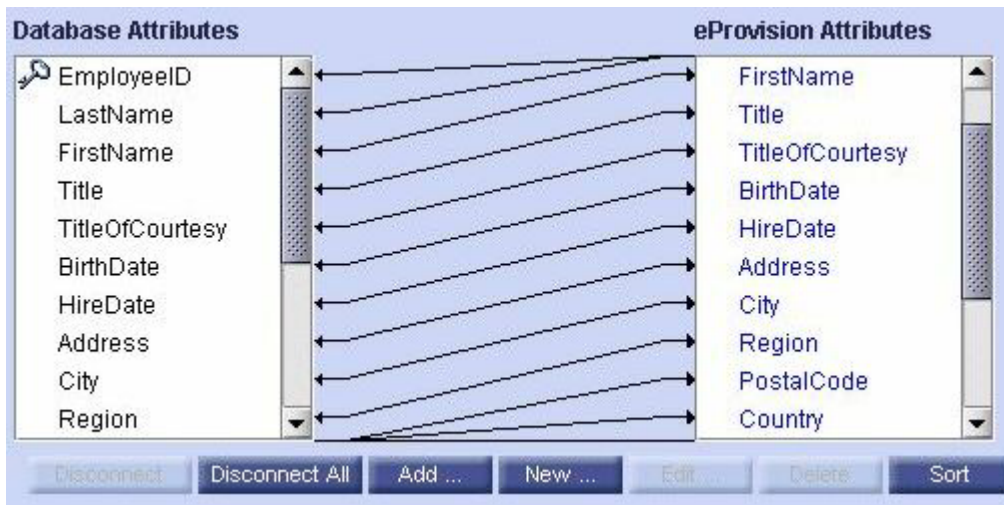
ePMs can be categorized, as follows:

- *Forward-type ePMs* – The business change request originates from the IdentityMinder eProvision system and propagates the change out to target systems that are managed by IdentityMinder eProvision.
- *Feeder-type ePMs* – Business changes that are made natively on the target system (e.g. HR admin changes user address in PeopleSoft™) are detected and synchronized with the profile data managed by IdentityMinder.
- *Bidirectional ePMs* – User profile data managed by IdentityMinder eProvision and any target resources can be synchronized in either direction. Most out-of-the-box ePMs are bi-directional.

A complete list of supported ePMs can be downloaded from the Netegrity support Web site at: <http://support.netegrity.com>.

## Data Synchronization

The data synchronization capabilities of IdentityMinder eProvision greatly simplify the process of administering users across a variety of resources and applications. During the process of configuring a resource connector, an administrator can designate what user attributes should be synchronized from the master identity store with the target resource. The attribute mapping process is done when configuring a resource connector. For connectors that are built using the ePM Xpress tool, the resource administrator is able to graphically map attributes from the master identity store to resource-specific attributes that are exposed by the managed system. The figure below illustrates the mapping process.



**Figure 4: Example attribute mapping process for a database ePM connector.**

## Reverse (Bi-directional) Synchronization

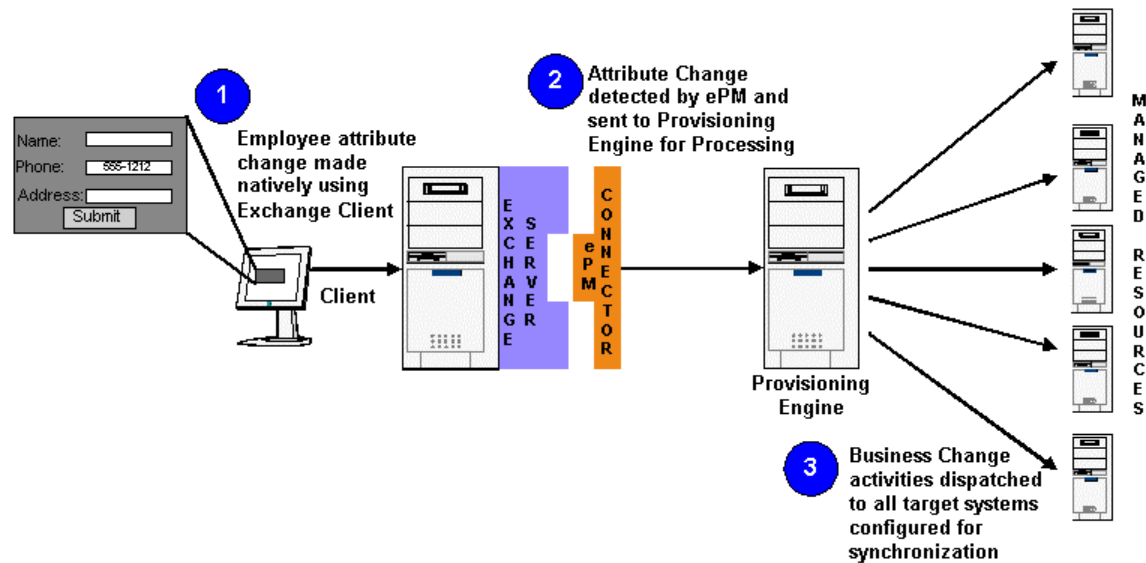
An important component of what an identity management and resource provisioning solution needs is the ability to deal with local changes made natively on target systems. This provides consistent and secure access to corporate resources by guaranteeing that the policies you have defined are applied to all changes, not just the ones made by the provisioning engine.

For example, when an IT administrator or end user manually modifies an attribute or other application-specific account information (e.g. phone number) directly on a target system that is managed by the provisioning engine (e.g. email account), the provisioning engine detects the change initiated by the target system, and determines the resource impacts (e.g. evaluate provisioning policies). If the attribute that was modified is configured for synchronization across multiple resources, a new business change is initiated by the provisioning engine, which may cause a series of update activities on any systems that are configured for synchronization.

### Reverse Synchronization Process Example:

1. User updates their phone number attribute in an Exchange email client application. The Exchange server is managed by the provisioning engine and is configured for synchronization with the master identity store and several other systems. The Exchange address book is configured as the "authoritative source" for the phone number attribute.

2. The ePM connector for Exchange detects the attribute change and sends a notification event to the provisioning engine.
3. The provisioning engine evaluates its policies to determine whether or not the attribute change initiated by Exchange requires an update to the master identity store. The master identity store (directory) is updated with the new phone number. The dynamic business rules engine evaluates its rules to determine whether or not additional synchronization activities need to execute. All managed systems that are configured for synchronization are informed of the changes to make, based on the rules already defined. The provisioning engine sends an update business change to the corresponding ePM connectors for each managed system to execute the attribute update. The attribute is updated across all managed systems configured for synchronization.



**Figure 5 – Reverse Synchronization Process**

By routing all changes through the dynamic business rules engine and thus forcing the use of its resource allocation policies, you maintain tight control over the allocation of resources, and help ensure that inadvertent security breaches are avoided.

The dynamic business rules engine allows any event to be managed automatically by a policy or manually by an authorized user. In both cases, the available options are as follows:

- ☐ The system can evaluate the data and determine that no actions need to be taken.
- ☐ The system can determine that the change was inappropriate for any reason (made by an unauthorized user, not within policy, etc), reject the change, and revert to the previous state.
- ☐ The system can determine that the change was appropriate and propagate the change to other systems including the master identity store.
- ☐ The system can determine that the change should be reinterpreted as a business change trigger and resubmit it for further processing. An example of such an event could be manually removing an employee from Exchange Server A to Exchange Server B to accommodate a job relocation. If the employee did not previously have an account on Exchange Server B, the provisioning engine can be authorized to reinterpret the action as equivalent to a trigger from an HR system.

Netegrity's data synchronization capabilities use a polling mechanism at the agent that is fully configurable. Depending on the type of system being configured for reverse synchronization, the agent does not necessarily have to be on the target system, and can use a number of network protocols to access the target system. When a change is detected, and the reporting interval has expired, the agent sends a message asynchronously to the provisioning engine for processing.

Both the polling interval and the reporting interval are configurable on a per target system basis.

## Progress Monitoring

You can monitor the progress of all pending activities and relieve bottlenecks as they occur. The status of each task is displayed in real time and denoted by different icons. Each provisioning task can optionally be configured for workflow approval, notification, and escalation. Upon completion of a provisioning task, its state is set to "Archived", which means that task has successfully completed. The status of all provisioning tasks is written to the audit database, which can then leverage the built in reporting capabilities included with IdentityMinder eProvision to generate detailed custom reports.



The screenshot shows a web interface titled "Bob Parker" with a sub-header "Choose action for selected activities". Below this is a table with columns: Status & Action, Activity Type, Activity Name, User Name, Target Date, and Activity Holder. The table lists eight activities, with the first one, "New Employee", highlighted in blue. A "Running" tooltip is visible over the first activity's status icon. At the bottom left, it says "8 activities found".

Status & Action	Activity Type	Activity Name	User Name	Target Date	Activity Holder
		<a href="#">New Employee</a>	<a href="#">Bob Parker</a>	Jun-4-2003	
		<a href="#">Create Exchange 2000 Account</a>	<a href="#">Bob Parker</a>	---	
		<a href="#">Open Exchange 2000 Account</a>	<a href="#">Bob Parker</a>	---	
		<a href="#">Welcome Email</a>	<a href="#">Bob Parker</a>	---	
		<a href="#">hrdummy - Create Record</a>	<a href="#">Bob Parker</a>	---	
		<a href="#">Welcome Letter</a>	<a href="#">Bob Parker</a>	---	
		<a href="#">Create Windows 2000 Account</a>	<a href="#">Bob Parker</a>	---	
		<a href="#">Open Windows 2000 Account</a>	<a href="#">Bob Parker</a>	---	

**Figure 6: Provisioning Engine Activity Manager**

## Auditing

IdentityMinder eProvision records all activities occurring in the system, storing the resulting information in a relational database. The activity information is particularly valuable to trace general and specific activities within identity environments to ensure there are no irregular or inefficient uses of the system. IdentityMinder eProvision itself uses the audit information to generate reports ([see next section](#)).

IdentityMinder eProvision's auditing capabilities become even more important in assessing a company's compliance with existing and upcoming government regulations addressing privacy, security, and disclosure. The Healthcare Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and the European Union Data Protection Directive are just some of the regulations that companies must adhere to. With IdentityMinder collecting security activity data automatically, you can assess your level of compliance with different regulations.

## Reporting

With the ability to delegate IdentityMinder eProvision tasks and activities, the ability to review reports of activities becomes critical. Central administrators need to assess on a regular basis how IdentityMinder eProvision is being used and whether users are receiving top-notch service. In addition, they also must ensure that IdentityMinder eProvision is being used properly.

IdentityMinder eProvision can generate reports on all IdentityMinder eProvision activities. The product includes several out-of-the-box reports providing lists of available roles, role definitions, role assignments of roles to users, when roles were assigned, and so on. Using reports, administrators can quickly gather data and review it.

Netegrity provides the schema for the database, thus administrators can create custom SQL queries to extract information on any activity they are interested in. Administrators can also delegate report generation to any other IdentityMinder eProvision administrator. IdentityMinder eProvision ensures that delegated reports display only information that the specific administrator has permission to view.

The provisioning engine itself provides a flexible web interface with a complete set of filters for generating detailed audit reports for the provisioning engine. The following diagram displays a sample report showing a list of provisioning activities for a given day.

Jun-17-2003						
Time Stamp	Category	Event Name	Event Status	Severity	User Name	Message
6/17/2003 7:06:09 AM	Provisioning	<a href="#">Business Change start</a>	In Progress	Info	Cat Fisher	
6/17/2003 7:08:07 AM	Provisioning	<a href="#">New resource</a>	Successful	Info	Cat Fisher	
6/17/2003 7:09:14 AM	Provisioning	<a href="#">New resource</a>	Successful	Info	Cat Fisher	
6/17/2003 7:10:00 AM	Provisioning	<a href="#">Business Change completion</a>	Successful	Info	Cat Fisher	
6/17/2003 7:12:30 AM	Provisioning	<a href="#">Business Change start</a>	In Progress	Info	Cat Fisher	
6/17/2003 7:13:00 AM	Provisioning	<a href="#">Resource update</a>	Successful	Info	Cat Fisher	
6/17/2003 7:13:02 AM	Provisioning	<a href="#">Business Change completion</a>	Successful	Info	Cat Fisher	
6/17/2003 7:31:45 AM	Provisioning	<a href="#">Business Change start</a>	In Progress	Info	Cat Fisher	
6/17/2003 7:32:41 AM	Provisioning	<a href="#">Resource removal</a>	Successful	Info	Cat Fisher	
6/17/2003 7:32:57 AM	Provisioning	<a href="#">Resource removal</a>	Successful	Info	Cat Fisher	
6/17/2003 7:33:02 AM	Provisioning	<a href="#">Resource removal</a>	Successful	Info	Cat Fisher	
6/17/2003 7:33:06 AM	Provisioning	<a href="#">Business Change completion</a>	Successful	Info	Cat Fisher	
6/17/2003 8:58:35 AM	Authentication	<a href="#">Control panel login</a>	Successful	Info		Login:Administrator
6/17/2003 9:08:30 AM	Authentication	<a href="#">Control panel logout</a>	Successful	Info		Logout:Administrator
6/17/2003 12:39:09 PM	Provisioning	<a href="#">Business Change start</a>	In Progress	Info	Babe Ruth	
6/17/2003 12:41:37 PM	Provisioning	<a href="#">New resource</a>	Successful	Info	Babe Ruth	
6/17/2003 12:42:46 PM	Provisioning	<a href="#">New resource</a>	Successful	Info	Babe Ruth	
6/17/2003 12:43:31 PM	Provisioning	<a href="#">Business Change completion</a>	Successful	Info	Babe Ruth	
6/17/2003 12:51:51 PM	Provisioning	<a href="#">Business Change start</a>	In Progress	Info	Babe Ruth	
6/17/2003 12:52:21 PM	Provisioning	<a href="#">Resource update</a>	Successful	Info	Babe Ruth	

**Figure 7: Sample audit report based for all activities performed on a given day.**

## Summary

The abundance of information technology in use at modern-day organizations presents a daunting administrative challenge for both business managers and IT departments. Managers expect that access to critical resources like email or ERP applications will be granted to those needing it as quickly as possible – and later be modified or revoked just as quickly, as job responsibilities change. IT departments need to manage privileges to more resources, for more users, in less time, often with limited staff – all while ensuring that increasingly complex security policies are being properly enforced.

Netegrity IdentityMinder eProvision helps organizations address these challenges with a solution that delivers timely, secure access to corporate resources for employees, as well as customers and partners, in a way that simplifies IT resource administration. IdentityMinder eProvision manages the administration of user access to enterprise applications, networks, databases and other essential resources, enabling managers to transform business changes (such as employee hiring/firing, or business alliances) into specific, automated IT activities – thereby increasing productivity, responsiveness and enforcing security policies more effectively.